REMARKS

This application has been carefully considered in connection with the Examiner's Final Office Action dated January 9, 2008. Reconsideration and allowance are respectfully requested in view of the following.

Applicants respectfully submit that the Office Action has omitted Claims 16 and 22 from the list of pending Claims. In the Office Action dated February 9, 2007 a restriction requirement was made. In response to this restriction requirement, Applicants elected on February 19, 2007 to prosecute Group I which comprised Claims 1-18 and 22-24. Applicants further elected Species IA of Group I, which comprised Claims 2-9, 17-18, and 23-24. Claims 1, 16, and 22 were identified as generic. Accordingly, Applicants elected to prosecute claims 1-9, 16-18, and 22-24. Applicants respectfully submit that Claims 16 and 22, generic claims to Species IA, are still pending and have not been withdrawn or canceled. Claims depending from both Claims 16 and 22 were rejected in the current Office Action without a corresponding rejection of Claims 16 and 22. Applicants believe the omission of these claims from the Office Action is a typographical error, and request correction of said error in the next Office Action.

Summary of Rejections

Claims 1-9, 16-18 and 22-24 were pending at the time of the Final Office Action.

Claims 1-9, 17-18 and 23-24 were rejected under 35 U.S.C. §103.

Claims 16 and 22 were not rejected or allowed.

Summary of Response

Claims 1, 16, and 22 are currently amended.

Claims 2-9, 17-18, and 23-24 remain as originally submitted.

Claims 10-15 and 19-21 were previously withdrawn.

Summary of Claims Pending

Claims 1-9, 16-18 and 22-24 are currently pending following this response.

Applicants Initiated Interview

Applicants thank Examiner Sherr for her time and consideration of the arguments presented in the personal interview on February 19, 2008. In the interview several claim amendments were discussed. For the purpose of clarity, and to further prosecution, the Claims have been amended consistent with discussions during the in person interview.

In the previous Office Action, a number of the limitations within the Claims were not discussed due to language which was interpreted by the Office Action as either being optional or not limiting due to being found in the preamble. For the sake of clarity, and without limiting the scope of the Claims, the Claims have been amended to positively recite all limitations and to include relevant limitations of the preamble within the body of the Claims. Therefore, similar arguments to those made in the response filed August 16, 2007 are respectfully reiterated herein. Applicants request that all of the limitations, including those which were previously not considered due to optional language or due to the language only being found in the preamble, be considered in the next Office Action.

Response to Rejections

Data migration from a first system to a second system is a difficult and time consuming process. The data being migrated may include user information with one or more encrypted data elements. For example, password data may be encrypted to protect the privacy of a user. These encrypted data elements may not be easily decrypted for a number of reasons, including the unavailability of decryption keys. Therefore, alternative solutions to obtaining encrypted data elements during migration are needed. The pending disclosure teaches systems and methods for data migration from a first system to a second system using data intercepted by a user.

Data migration as described throughout the pending disclosure, including paragraphs [0017]-[0026], and as used herein refers to the process by which data is moved from one proprietary system to another proprietary system. For example, the proprietary system by one vendor may store encrypted data using one proprietary encryption scheme while another vendor may use a different proprietary encryption scheme. The data migration process is not simply the copying of data from one source datastore to a target datastore, but rather includes the gathering of data from a source datastore in a first format, converting some or all of the data in the first format to a second format of the target datastore, and then saving the converted data in the second format on the target datastore. In addition, data migration requires that encrypted data elements of the source datastore, such as encrypted password information, which cannot be easily decrypted by the target datastore, be obtained from the user and added to the target datastore. For example, the target datastore may not have decryption keys for decrypting encrypted data elements of the source datastore. Obtaining encrypted data elements of the source datastore from the user maintains consistency between the contents of the source datastore and the target datastore. This two step process overcomes many of the prior art limitations and does not require the decryption of the source datastore by the target datastore.

As disclosed in Paragraph [0021], intercepting data may refer to the process by which a user sends password data intended for the source datastore and the target datastore intercepts the password data. Accordingly, user password information which is stored as encrypted user password information on the source datastore is obtained without decrypting the encrypted user password information on the source datastore. Unlike packet sniffing, interception includes obtaining the password data, verifying the password data, and storing password data in the target datastore. The user password data is intercepted directly from the user and can be verified using the source database. This verification occurs by having the target datastore send the password data to the source datastore, and the source datastore confirming that the password data is valid. Therefore, the target datastore performs the data interception by acting as an intermediary between a user and the source datastore. As described above, encrypted password data may be captured and provided to the target datastore using the interception process, thereby allowing for user passwords and other encrypted data to be migrated from a first proprietary system to a second proprietary system without having every user re-enter their security information.

Blakley, III et al. (U.S. Patent No. 5,832,211, "*Blakley*") relates to a network system server that provides password synchronization between a main datastore and a plurality of secondary datastores so that a user is able to maintain a single, unique password among the plurality of secondary datastores. Blakely uses a password synchronization server to store user names and plain-text passwords securely and to respond to requests from secondary datastores for their retrieval. The passwords are sent to the secondary datastores using encryption that is decipherable by the secondary datastores. Blakely does not teach or suggest migrating data from a source datastore to a target datastore, and does not address the problem of migrating from one vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information.

Mehring et al. (U.S. Patent No. 6,609,115, "*Mehring*") relates to a method of allowing a remote system user to request multiple software applications using a single log-in. Although the remote user is only required to log-in once, the user information is submitted to the policy server every time the remote user logs-in to a different web server. Like *Blakley*, *Mehring* does not teach or suggest migrating data from a source datastore to a target datastore, and does not address the problem of migrating from one vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information. It is respectfully submitted that *Mehring* does not cure the deficiencies of *Blakley.*

Densmore (U.S. Patent No. 6,591,305, "*Densmore*") relates to a method of delivering content to a web browser. Like *Blakely* and *Mehring*, *Densmore* does not teach or suggest migrating data from a source datastore to a target datastore, and does not address the problem of migrating from one vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information. *Densmore* does not cure the deficiencies of the art of record.

These distinctions, as will other distinctions, will be discussed in more detail in this paper.

Response to Rejections under Section 103

Claim 1:

In the January 9, 2008 Office Action, Claim 1was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Blakley* and further in view of *Mehring* and further in view of *Densmore.*

I. *Blakley* is directed towards clear-text passwords synchronization of server data within a closed network, not "migrating from a source user authenticator having a source datastore containing encrypted password data and other unencrypted data" as claimed.

Blakley is limited to the transmission of clear-text data. (*Blakley*, Col. 10, ll. 46-67). The servers of *Blakley* are limited to the synchronization of data using this clear-text data. Clear-text data is information which is sent in the "clear" with no encryption.

In contrast, Claim 1 recites "a method for migrating from a source user authenticator having a source datastore containing ***encrypted password data*** and other unencrypted data" [emphasis added]. Therefore, unlike *Blakley*, Claim 1 intercepts password data from an end user without the need to decrypt encrypted information or obtain encrypted information from the source user authenticator from which data is being migrated. None of the art of record teaches or suggests the use of intercepted data. Therefore, it is respectfully submitted that the limitations of Claim 1 are not obvious.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest a mechanism which allows for the interception of data from an end user such that encrypted data may be migrated from a source user authenticator to a target user authenticator.

II. *Blakely* does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that locates a corresponding identification in a target datastore and determines whether the target datastore includes a password associated with the identification.

Claim 1 recites, "A method for migrating from a source user authenticator … to a target user authenticator … comprising … Implementing a servlet that … Locates the corresponding identification in the target datastore and … Determines the target datastore does not include a password associated with the identification".

The Office Action appears to suggest that the foreign registries of *Blakely* locate a corresponding identification in their target datastore. However, Applicants are unable to find such a teaching in *Blakely*. The section of *Blakely* cited in support of this suggestion (Col. 11, lines 44-55) describes the requirements met by the password synchronization function. The requirements do not include locating a corresponding identification in their target datastore and determining whether their datastores include a password associated with the identification. It is not necessary for the foreign datastores of *Blakely* to determine if their datastores include a password associated with an identification because they are networked with the main datastore. Their datastores are configured to be propagated immediately with any changes to passwords in the DCE datastore. Col. 11, lines 27-32 of *Blakely* states:

> … synchronization causes passwords changed by DCE users to be propagated as plaintext passwords **to any** other foreign registry configured to receive such changes. **Propagation is immediate**, with results saved for retry, as necessary, should communications with the foreign registries be broken. (Emphasis added by Applicants.)

Therefore, no determination is made by the foreign registries. They simply receive any changes made to the DCE passwords.

The pending disclosure discloses a method to port user data out of the proprietary and/or encrypted datastore of the old authenticator and into the new datastore for the new authenticator while minimizing the impact on the user experience. This allows for the transitioning from one authenticator to the next for the protection of web resources with minimal impact to applications or users. *Blakely* does not address the problems associated with migrating data from one vendor's proprietary database schema to another vendor's product and does not teach or suggest the solution disclosed in the pending disclosure.

Accordingly, Applicants respectfully submit that *Blakely* does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that locates the corresponding identification in the target datastore and determines that the target datastore does not include a password associated with the identification.

III. *Mehring* does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that submits the received identification and received password to the source user authenticator when the target datastore does not include a password associated with the identification.

Claim 1 also recites, "A method for migrating from a source user authenticator … to a target user authenticator … comprising …determines that the target datastore does not includes a password associated with the identification".

The Office Action appears to suggest that the authentication step described in *Mehring* discloses submitting the received identification and received password to the source user **when** the target datastore does not include a password associated with the identification. However, as stated earlier, *Mehring* does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator. Instead, *Mehring* describes a method for allowing a remote system user to request multiple software applications using a single log-in. More importantly, as stated in the section of *Mehring* cited in the Office Action (Col. 10., line 49 – Col. 11, line 10), although the remote user is only required to log-in once, the user information stored in the web browser log-in cache is submitted to the policy server every time the remote user logs-in to a different web server. Therefore, having user information stored in the web browser log-in cache does not eliminate the need to submit the user information to the policy server every time the remote user logs-in to a different web server. It only eliminates the need of having the remote user log-in separately to different web servers. By contrast, in the present application, once a password is associated with an identification in the target datastore, there is no longer a need to submit the request to the source user authenticator.

Accordingly, Applicants respectfully submit that *Mehring* does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that submits the received identification and received password to the source user authenticator **when** the target datastore does not include a password associated with the identification.

IV. The system and method of the pending disclosure populates the target datastore with the received password from the user. It does not populate the target datastore with the password from the source user authenticator.

Claim 1 further recites, "A method for migrating from a source user authenticator … to a target user authenticator … comprising … populates the target datastore with the received password associating the received password with the corresponding identification."

The Office Action noted that *Blakely* does not disclose this element. However, the Office Action suggested that:

> It would have been obvious to one having ordinary skill in the art at the time of the invention was made to on receipt of an approval response from the source user authenticator populate the target datastore with the received password associating the received password with the corresponding identification, since it is known in the art to facilitate the complete transfer of data, when data is found missing from the original source, it is restored by the data from the original source. (Page 7, January 9, 2008 Office Action)

Applicants are unclear as to how data can be restored from the original source if it is missing from the original source. If the Office Action is suggesting that the target datastore of the pending disclosure is populated with passwords from the source datastore, Applicants respectfully submit that this understanding incorrectly reflects the claimed subject matter. The claims call for using the received password (received from the User) to populate the target datastore. For the reasons stated earlier, the target datastores cannot be populated with passwords from the source datastore by simply propagating passwords from one datastore to another because the password in the source database may be encrypted and the target database may not be able to decrypt the password from the source database. That is why it is necessary to receive the password from the user and not the source datastore. The system and method of the present application waits for the approval response from the source user authenticator before populating the target datastore with the password entered by the user as a way of verifying if the identification and password entered by the user are valid, not as a way of restoring missing data.

The combination of *Densmore* with aforementioned references also fails to teach populating a datastore with user password information. The migration of user data using an servlet or interceptor is not taught or suggested by *Densmore*.

Furthermore, *Densmore* does not disclose the presently claimed invention since *Densmore* directs one to provide data to a user rather than intercept data from a user as in the pending disclosure. *Densmore* teaches delivering content to users, not delivering information to a datastore (Col 4, ll. 28-34). Thus, one of ordinary skill in the art would not be motivated to make the changes proposed by the Office Action.

Neither of the cited references, singly or in any motivated combination thereof, address the problems associated with migrating data from one vendor's proprietary database schema to another vendor's product and do not teach or suggest the solution disclosed in the present application. Accordingly, Applicants respectfully submit that the teachings of these references would not suggest the claimed subject matter to a person of ordinary skill in the art.

Claims Depending From Claim 1:

Claims 2-9 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Blakley* and further in view of *Mehring* and further in view of *Densmore*.

Dependent Claims 2-9 depend directly or indirectly from independent Claim 1 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-IV above, Applicants respectfully submit that Claims 2-9 are not taught or suggested by *Blakley* in view of *Mehring* and further in view of *Densmore* and respectfully request allowance of these claims.

Claim 16:

Claim 16 was not explicitly rejected in the Office Action. While Applicants note that no rejection is currently pending as to Claim 16, Applicants respectfully submit that Claim 16 contains limitations substantially similar to the limitations discussed in sections I-IV above. For at least the reasons established above in sections I-IV, Applicants respectfully submit that independent Claim 16 is not taught or suggested by *Blakley* in view of *Mehring* and further in view of *Densmore* and respectfully request allowance of this claim.

Claims Depending from Claim 16:

Claims 17-18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Blakley* and further in view of *Mehring* and further in view of *Densmore*.

Dependent Claims 17-18 depend directly or indirectly from independent Claim 16 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-IV above, Applicants respectfully submit that Claims 17-18 are not taught or suggested by *Blakley* in view of *Mehring* and further in view of *Densmore* and respectfully request allowance of these claims.

Claim 22:

Claim 22 was not explicitly rejected in the Office Action. While Applicants note that no rejection is currently pending as to Claim 22, Applicants respectfully submit that Claim 22 contains limitations substantially similar to the limitations discussed in sections I-IV above. For at least the reasons established above in sections I-IV, Applicants respectfully submit that independent Claim 22 is not taught or suggested by *Blakley* in view of *Mehring* and further in view of *Densmore* and respectfully request allowance of this claim.

Claims Depending from Claim 22:

Claims 23-24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Blakley* and further in view of *Mehring* and further in view of *Densmore*.

Dependent Claims 23-24 depend directly or indirectly from independent Claim 22 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I-IV above, Applicants respectfully submit that Claims 23-24 are not taught or suggested by *Blakley* in view of *Mehring* and further in view of *Densmore* and respectfully request allowance of these claims.

Conclusion

Applicants respectfully submit that the present application is in condition for full allowance for the reasons stated above, and Applicants respectfully request such allowance. If the Examiner has any questions or comments or feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 21-0765, Sprint.

Respectfully submitted,

Date: March 7, 2008

/Michael W. Piper/
Michael W. Piper
Reg. No. 39,800

ATTORNEY FOR APPLICANTS

CONLEY ROSE, P.C.
5601 Granite Parkway, Suite 750
Plano, Texas 75024
(972) 731-2288
(972) 731-2289 (facsimile)